양자 통신 및 양자 암호의 개요

손일권, 이성훈, 박주윤, 허준
고려대학교

요 약

정보통신망에서 개인정보의 유출로 인한 사회문제가 최근에 큰 이슈가 되면서 정보통신의 보안 기능이 더욱 주목을 받고 있다. 차세대 통신 기술은 정보의 전송 속도나 전송 효율성보다 정보의 보안성에 더 큰 방점이 있을 것이라는 예상도 나오고 있다. 정보보호의 기초는 암호화와 복호화를 통하여 정보가 노출되어도 원래의 정보를 파악 할 수 없도록 만드는 것이며 암호화와 복호화를 위한 암호키의 생성 및 관리 기술의 발전이 곧 암호 및 정보보안 기술의 발전과 궤를 같이 한다. 본 논문에서는 암호키 관리의 새로운 패러다임으로 최근에 주목을 받고 있는 양자 암호의 원리를 소개하고 이를 바탕으로 양자통신의 미래를 예상한다. 또한 양자 암호와 양자통신 기술을 뒷받침하는 다양한 양자 정보 처리기술의 현황에 대해서도 간략하게 살펴본다.

Ⅰ. 서 론

양자통신은 양자상태에 담겨있는 정보를 송신 측에서 수신 측까지 전달하는 과정을 의미하며 이 때 양자상태에 담겨있는 정보는 0 또는 1의 이진 정보일 수도 있고 0 과 1이 중첩되어 있는 정보일 수도 있다. 특히 0 과 1 의 이진정보를 양자상태에 실어서 보내는 양자통신의 경우에 전송되는 이진정보를 누군가가 도청하게 되면 수신자는 즉각 도청자의 존재를 인식하게 되고 따라서 통신을 중단한 후 상황에 알맞은 대처를 하게 된다. 이러한 특성을 암호키 전송에 응용한 것이 양자암호이며 암호화와 복호화를 위한 암호키를 송신자와 수신자가 나누어 가지게 된다는 의미에서 양자암호키분배 즉 QKD(Quantum Key distribution) 이라고 부른다. 넓은 의미에서의 양자 통신은 0 과 1이 중첩되어 있는 양자상태를 송신부에서 수신부로 전송하는 모든 기술을 일컫는다. 하지만 암호키를 비롯하여 현재 우리가 정보의 형태로 인식하는 영상, 음성, 문자 등은 모두 이진정보로 표현되므로 현대 통신에서 0과1의 중첩상태가 의미 있는 정보로 인식되는 경우는 매우 제한적이기 때문에 현재까지는 양자 통신이 좁은 의미로써 양자 암호와 동일한 의미로 사용되고 있다. 본 논문에서는 양자통신의 두 가지 경우를 모두 다루고 있으며 이후부터는 이진정보를 전송하는 경우는 양자 암호로 부르고 중첩정보를 전송하는 경우를 양자통신으로 부르기로 한다.

본 논문에서는 물리적 원리 및 수학(정보 이론)을 기반으로 한 양자 암호의 개요에 대하여 살펴본 후에 양자통신과 관련된 주요 기술인 양자컴퓨터, 양자 오류 정정 부호 및 양자 난수 발생기와 양자 라이더에 대하여 고찰한다.

Ⅱ. 본 론

1. 양자 키 분배 프로토콜

기존의 RSA 암호체계는 소인수 분해 알고리즘의 계산 복잡도를 기반으로 하고 있으므로 기존의 컴퓨터에 비해서 연산 속도가 월등히 빠른 양자 컴퓨터가 개발되면 키 분배 과정에서 도청으로 인하여 키를 알아 낼 위험성이 있다. 양자의 불확정성의 원리에 기반한 양자 키 분배는 도청의 위험성이 없는 키 분배 과정이다.

정보이론의 측면에서 정보를 전달하는 단위가 비트였다면, 양자 정보 이론에서는 정보의 단위로 양자비트, 즉 큐비트로 나타낸다. 양자 키 분배를 구현할 때 큐비트를 구현하는 방법으로 단일 광자를 이용한다. 광자는 서로 거의 상호작용을 하지 않고 장거리 통신에 강한 장점이 있다.

양자 키 분배 프로토콜 중에서 대표적인 방법으로 BB84프로토콜이 있다. BB84프로토콜은 Bennett와 Brassard가 1984년에 제안한 프로토콜로 불확정성의 원리에 기반하여 키 분배 과정에서 송신자 Alice가 수신자 Bob에게 보낸 정보를 도청자 Eve가 도청을 시도했을 때 Bob이 수신하는 정보에 도청의 흔적이 남으므로 Bob은 도청 사실을 알 수 있다. BB84 프로토콜의 개요는 다음과 같다.

Alice가 랜덤 한 비트 수열을 정하고 각각의 비트를 편광 시킬 편광 판 또한 임의로 고른다. 결정한 두 랜덤 수열을 바탕으로 각각의 랜덤 한 비트를 편광 시켜서 Bob에게 전송한다.

표 1. 편광판에 따른 비트의 편광결과

	십자형	대각형
0	–	／
1	|	＼

표 2. 랜덤 수열에 의한 편광 판의 비트 표시

0	십자형
1	대각형

Bob은 임의의 편광 판을 사용하여 전송된 광자를 측정한다. 이 때 Alice가 보낸 광자 중 일부는 양자채널의 잡음 등의 이유로 손실되어 Bob이 수신하지 못할 수 있다.

표 3. 전송된 광자를 측정한 결과

Bob 수신 편광 Alice 전송 신호	십자형	대각형
–	–	／ 또는 ＼
|	|	／ 또는 ＼
／	– 또는 |	／
＼	– 또는 |	＼

이와 같이 양자채널을 이용해서 이루어지는 양자 정보의 전송 과정이 끝난 후에는 공개채널을 통해서 서로 동일한 비밀 키를 나누기 위한 후처리 과정이 요구된다..

Bob은 Alice에게 자신이 어떤 광자를 수신했는지에 대한 정보를 전송하고 그 위치의 편광 판 정보를 함께 알려준다. Alice도 Bob이 수신한 광자에 해당하는 위치에 대한 편광 판 정보를 알려준다. Alice와 Bob은 각각 전송 받은 편광 판 정보를 바탕으로 서로 같은 편광 판을 쓴 정보만을 모은다. Bob은 걸러낸 수열 중의 일부를 공개하는데 공개한 수열이 Alice가 전송한 수열과 같으면 Bob이 공개하지 않은 나머지 수열을 비밀키로 사용한다.

잡음이 없는 채널과 도청이 없는 상황을 가정한다면 서로 나눈 비밀 키가 동일하지만 실제로 쓰이는 채널은 잡음이 존재하고 도청도 존재 할 수 있다. 채널의 잡음을 고려한다면 성공적으로 비밀 키를 공유해도 잡음에 의해 오류가 날 확률이 존재한다. 오류가 날 확률은 표본으로 뽑은 임의의 비트 중 오류가 난 비트의 비율로 다음과 같다.

$$R_m = \frac{\text{오류난 비트}}{\text{표본 비트}} \quad (1)$$

R_{max}을 허용 가능한 최대의 오류확률이라 할 때, R_m이 오류의 최대치 R_{max}를 넘지 않으면 비밀 키로 사용하고 R_{max}를 넘으면 도청이 있었던 것으로 간주하고 비밀 키 공유를 다시 시작한다.

2. BB84 프로토콜의 예시

(1) Alice가 각각 랜덤 한 수열 두 개를 생성한다.

예시: 랜덤 한 두 수열

비트 정보	0	1	0	0	1	1	1	0	1	0
편광판 정보	0	1	1	0	1	0	1	1	1	0

(2) 편광 판으로 편광 한 광자를 Bob에게 보낸다.

예시: 편광 된 광자 전송

편광된 광자	–	＼	|	–	＼	|	＼	／	＼	–

(3) Bob은 Alice에게 받은 광자를 임의로 정한 편광 판 순서대로 측정한다. 예시에선 첫 번째와 다섯 번째로 전송된 광자를 수신하지 못한 상황이다.

예시: 광자 측정

편광판 정보	1	1	0	1	1	0	0	1	1	1
측정한 광자	×	＼	|	＼	×	|	–	／	＼	／

(4) Bob은 어떤 광자를 받았는지에 대한 정보를 Alice에게 전송하고, 그 광자를 측정하는데 사용한 편광 판 정보도 전송한다.

예시: 수신한 광자 위치정보와 편광 판 정보 전송

수신한 광자위치	2	3	4	6	7	8	9	10
편광판 정보	1	0	1	0	0	1	1	1

(5) Alice는 Bob이 측정한 광자의 위치에 대응하는 Alice의 편광 판 정보를 Bob에게 전송한다.

예시: 대응하는 위치에 대한 편광 판 정보 전송

편광판 정보	1	1	0	0	1	1	1	0

(6) Alice와 Bob은 서로 같은 편광 판을 사용한 위치의 비트를 비밀키로 공유한다.

예시: 비밀키 공유

비밀키	1101

2. 양자 키 분배 후처리

양자 키 분배의 후처리(post-processing) 과정은 도청자의 공격 혹은 양자 채널과 양자 검출 장치의 불완전성으로 인해 발생하는 송수신자의 암호키 사이의 불일치를 해소하는 과정이다. 이를 통해 송수신자 사이의 동일한 키 정보를 보장하며, 동시에 도청자가 노출되는 정보로부터 키에 대한 정보를 유추하지 못하도록 노출되는 정보와 키 정보 사이의 상관관계를 최대한 낮출 수 있다. 이러한 후처리 과정은 정보보정(information

reconciliation), 비밀성증폭(privacy amplification) 그리고 인증(authentication) 과정으로 구성된다.

가. 정보보정

정보보정은 여러 가지 요인으로 인해 발생하는 송수신자 사이의 정보 불일치를 해소하여 동일한 정보를 가질 수 있게 만들어 주는 과정이다. 즉, 이동통신에서 수신자 정보의 오류를 정정하는 오류 정정 과정과 동일하다. 다만 미리 정보를 오류 정정을 위해 부호화하는 것이 아니라 송수신자 사이의 암호키 정보 전송이 끝난 후 추가적인 정보 전송을 통해 오류 정정을 수행한다. 이때 추가적인 정보 전송은 일반적인 인터넷 환경과 같은 오류율이 0인 공개 채널(public channel)을 통해 이루어지기 때문에 도청자에게 일정량의 정보가 누출되는 문제가 발생한다.

정보보정 프로토콜의 대표적인 예는 1994년 G. Brassard와 L. Salvail이 제안한 Cascade 프로토콜이다[1]. 이 프로토콜은 뛰어난 성능을 보임으로써 현재 정보보정 프로토콜 중에 사실상의 표준(de facto standard)으로 여겨진다.

Cascade 프로토콜은 이진 검색 (binary search) 알고리즘과 역 추적(trace back) 알고리즘으로 구성되며 여러 단계에 걸쳐 반복 진행된다. 각 단계마다 전체 암호키를 여러 블록으로 나누고 블록마다 이진 검색을 수행하고 패리티 정보를 송수신자가 비교하여 블록 내의 오류를 수정한다.

이진 검색은 한 블록 당 하나의 오류만 수정이 가능하기 때문에 남아있는 오류 정정을 위해 다음 단계로 넘어간다. 다음 단계에서는 암호키를 완전히 섞은 후 이전 단계보다 두 배 크기의 블록으로 나누어 이진 검색을 다시 수행한다.

2단계 이상부터 이진 검색이 끝난 후 역 추적을 수행한다. 이진 검색을 통한 오류 정정을 통해 그 이전 단계에서 드러나지 않았던 오류를 역으로 추적하여 정정하는 것이다. 이러한 두 과정이 연쇄적으로 일어나며 더 이상 오류를 찾을 수 없을 때 넘어간다. 다음 단계에서 두 알고리즘을 다시 똑같이 수행하며 오류를 더 이상 찾아낼 수 없는 단계에서 Cascade 프로토콜은 종료된다.

Cascade 프로토콜은 도청자에게 노출되는 정보량이 이론적인 한계치에 거의 근접하는 우수한 프로토콜이지만 여러 단계에 걸쳐 수행되며 지속적으로 정보를 주고 받기 때문에 통신 횟수가 매우 크다는 단점이 존재한다. 지속적이면서 매우 큰 통신 횟수는 실제 시스템에서 문제점으로 작용한다.

이러한 Cascade 프로토콜의 단점을 해소하기 위해 고안된 것이 Winnow 프로토콜이다. Winnow 프로토콜은 많은 부분에서 Cascade 프로토콜과 흡사하지만 이진 검색 알고리즘이 아

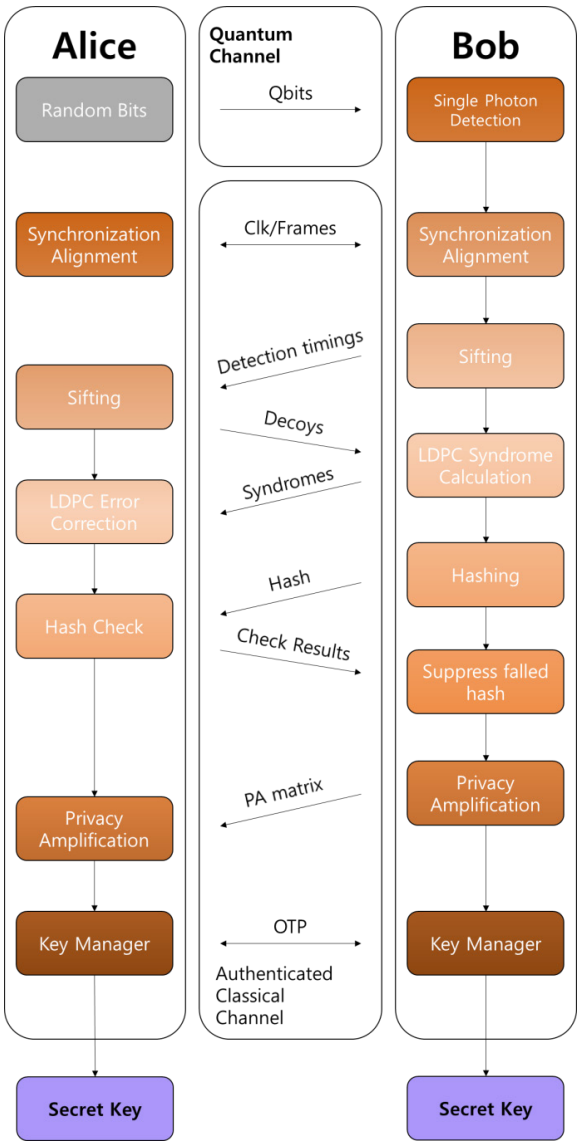

그림 1. 양자 키 분배 시스템

닌 널리 알려진 선형 부호인 해밍 부호를 이용한다. 이를 위해 Cascade 프로토콜처럼 전체 정보를 블록 단위로 나누지만 패리티 정보가 아닌 해밍 부호의 신드롬(syndrome) 정보를 주고받아서 오류를 정정한다. 이진 검색 알고리즘을 활용하지 않기 때문에 송수신자 사이의 통신 횟수는 대폭 줄어든다. 이로 인해 빠른 오류 정정이 가능하며 통신 채널의 부담이 줄어든다. 그러나 양자 채널의 오류율이 커질수록 도청자에게 노출되는 정보량이 Cascade 프로토콜보다 더 많아진다.

송수신자 사이의 채널 사용 횟수를 줄이면서 Cascade 프로토콜에 가까운 성능을 내기 위해 고안된 것이 LDPC 부호를 이용한 프로토콜이다. LDPC 부호는 오류 정정 부호 중 Shannon 한계에 근접했다고 알려져 있다. 이러한 LDPC 부호를 이용한

프로토콜의 가장 큰 장점은 송신자가 수신자에게 한 번의 추가 정보 전송만으로 오류 정정을 수행할 수 있다는 점이다. 즉, 단방향(One-way) 통신이 이루어진다. 이 때 전송되는 추가 정보는 패리티 검사 행렬을 통해 생성한 신드롬 정보이며 이 정보의 양이 도청자에게 노출된 정보량이 된다. LDPC 부호를 이용한 프로토콜의 단점은 다른 프로토콜과 다르게 실패할 확률이 있다는 점이다. Winnow프로토콜이나 Cascade 프로토콜의 경우 정보를 지속적으로 주고받으며 오류가 다 정정될 때까지 수행한다. 따라서 성공할 때까지 지속된다. 그러나 LDPC부호를 이용한 프로토콜의 경우 추가 정보를 한번만 전송하고 끝이기 때문에 고정된 정보를 통해 수신자는 오류 정정을 수행하여야 한다. 따라서 추가 정보를 통해 오류를 완벽히 정정할 수 있는지 없는지, 즉 성공 및 실패가 결정된다. 만약 실패했을 경우 피드백을 통해 이전에 전송했던 정보량보다 크기를 늘려 다시 전송하여 오류를 수정할 수 있다.

나. 비밀성 증폭

비밀성 증폭은 도청자가 가지는 정보와 암호키 정보 사이에 존재하는 상관관계(correlation)을 낮추는 과정이다. 정보보정 과정에서 오류를 암호키의 오류를 정정하는 과정에서 도청자에게 일정량의 정보를 노출하게 된다. 즉, 도청자가 암호키에 대해 일정량의 정보를 가지고 있기 때문에 완벽한 보안을 위해 노출되는 정보량만큼 암호키 정보에서 제거하게 된다.

1988년, Bennet, Brassard 그리고 Robert에 의해 비밀성 증폭의 개념이 처음 제안되었다[4]. 그 후 1995년 C. Crepeau와 U. M. Maurer와 합동으로 일반적인 비밀성 증폭의 개념을 제안하였다[5].

정보보정 과정을 거치게 되면 송수신자 사이의 공유된 암호키는 오류를 정정하기 위해 사용된 추가 정보가 도청자에게 노출되어 일부분만 완벽한 비밀성을 가지게 된다. 된다. 따라서 비밀성 증폭은 송수신자 사이에 공유된 암호키가 완벽한 비밀성을 가질 수 있도록 정보를 정제하는 과정이다.

송수신자 사이의 n비트 문자열의 확률 변수를 W, 도청자가 가지는 t비트 문자열의 확률 변수를 V라고 하자. 도청자는 상관관계를 가지는 확률 변수 V를 통해 W에 대한 정보를 최대 $t<n$ 비트의 정보를 알 수 있다. 즉 다음과 같은 관계가 성립된다.

$$H(W|V) \geq n - t$$

송신자와 수신자는 압축 함수 $g:\{0,1\}^n \rightarrow \{0,1\}^r$을 선택한다. 도청자는 자신의 가진 W에 관한 일부 정보와 고유의 정보를 조합하더라도 $K=g(W)$에 관해 매우 작은 정보량만을 얻을 수 있다. K는 도청자의 모든 정보를 통해 추측할 때 사실상 균등 분포나 다름없기 때문에 이는 안전하게 암호키로 활용될 수 있다. K의 길이 r은 도청자에게 노출되는 정보량에 의해 결정되는 값이다.

비밀성 증폭의 대표적인 방법 중 하나는 유니버설 해싱(Universal Hashing)이다. 해싱은 어떤 입력 값(일반적으로 문자열)을 가지고 작은 값(보통 테이블 내의 인덱스 조회)을 생성하는 데 사용되어 왔으며 이후 두 입력 값이 같은 값인지 확인하는 데에도 활용되었다. 따라서 해시 함수는 다대일(many-to-one) 대응(mapping)으로 볼 수 있다. 다대일 대응이기 때문에, 해시 함수 값들이 충돌하는 입력 값들이 반드시 존재한다. 이러한 해시 함수들 중 특정한 특성을 가지는 해시 함수 g를 선택하기 위한 확률적 알고리즘이 유니버설 해싱이다. 유니버설 해싱은 어떤 두 개의 서로 다른 입력 값 x,y에 대해 $g(x)=g(y)$일 확률이 최대 $\frac{1}{m}$(m은 해시 함수 치역의 크기)라는 특성을 가진다.

이러한 유니버설 해싱의 특성을 통해 도청자가 암호키에 대해 추정할 수 있는 확률을 현저히 낮출 수 있다. 서로 다른 입력 값을 암호 키의 압축 전 문자열과 도청자가 추정하는 암호 키의 문자열이라고 생각하면 해시 충돌이 발생할 확률이 최대 $\frac{1}{m}$이라는 매우 작은 값을 가진다. 따라서 해시 함수를 통해 길이가 줄어든 송수신자 사이에 공유된 암호키에 대해 도청자는 추정이 거의 불가능하다.

다. 인증

인증은 양자 키 분배만의 특별한 과정은 아니며 일반적으로 볼 수 있는 많은 인증 과정들과 동일하다. 인증은 일반적으로 도청자의 중간자 공격(man-in-the-middle attack)에 대처하기 위해 필요하다.

중간자 공격은 도청자가 송신자가 보낸 정보를 가로채 수신자에게 틀린 정보를 보내는 것이다. 따라서 수신자는 자신이 받은 정보가 정말 적법한 송신자에게서 온 것인지 확인이 필요하다. 이를 위해 송수신자 사이에 미리 약속된 해시 함수를 통해 송신자는 암호키에 대한 해시 태그를 생성해 암호키와 함께 보낸다. 수신자는 암호키를 자신이 가진 해시 함수에 입력해 생성한 해시 태그가 송신자가 보낸 해시 태그와 일치하는지 확인하여 적법한 송신자인지 확인할 수 있다.

따라서 인증 과정은 키 분배 후처리의 모든 과정에서 함께 수행된다. 정보보정 과정과 비밀성 증폭 과정에서도 송신자와 수신자 사이의 정보 전송은 인증과 함께 진행된다.

3. 양자 통신 관련 기술

가. 양자 컴퓨터

양자 컴퓨터는1982년 파인만에 의해 처음 제시되었다[6]. 파인만은 양자 컴퓨터의 구체적인 동작이나 알고리즘을 보인 것

은 아니지만 양자 시스템의 복잡한 현상들을 시뮬레이션 하기 위해서는 양자 컴퓨터가 필요함을 밝혔다.

현대 컴퓨터는 0,1의 값을 갖는 비트를 기본으로 데이터를 처리한다. 이에 비해 양자 컴퓨터는 0과 1의 중첩 상태를 가지는 큐비트를 이용한다. 비트와 다르게 수가 늘어나면 연산 가능한 공간이 지수적으로 증가하는 큐비트의 성질과 큐비트 간의 상호작용인 얽힘을 사용하면 양자 병렬 처리가 가능하게 되고 이를 통해 연산속도의 엄청난 향상이 가능하다. 이러한 양자 병렬 처리를 설명하기 위해 유니터리 연산 U_f를 다음과 같이 가정한다.

$$U_f|x\rangle|0\rangle = |x\rangle|f(x)\rangle \tag{3}$$

Walsh-Hadamard 변환 W_m을 통해 연산을 취해줄 2^m개의 모든 입력 값을 준비한다.

$$\begin{aligned} W_m|0\cdots 0\rangle &= \frac{1}{\sqrt{2^m}}(|00\cdots 0\rangle + |00\cdots 1\rangle + \cdots \\ &\quad + |11\cdots 1\rangle) \\ &= \frac{1}{\sqrt{2^m}}\sum_{x\in 2^m}|x\rangle = \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x\rangle \end{aligned} \tag{4}$$

여기에 결과값을 얻기 위한 연산을 해주게 되면 2^m개의 결과값을 동시에 계산할 수 있다.

$$\begin{aligned} U_f W_m|0\rangle &= U_f\left(\frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x,0\rangle\right) \\ &= \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}U_f|x,0\rangle \\ &= \frac{1}{\sqrt{2^m}}\sum_{x=0}^{2^m-1}|x,f(x)\rangle \end{aligned} \tag{5}$$

입력값 대한 측정을 함으로써 원하는 결과값을 얻을 수 있다.

이러한 양자 컴퓨터를 구현하기 위한 다섯 가지 조건[7]을 Divincenzo가 2000년도에 제시하였다.

(1) 명확하게 구별할 수 있는 큐비트를 가진 확장 가능한 시스템이어야 한다.

(2) 와 같이 기준이 될 수 있는 양자 상태를 만들 수 있어야 한다.

(3) 연산에 사용되는 큐비트들이 양자 컴퓨터의 게이트들의 연산 시간보다 더 긴 relevant decoherence 시간을 가져야 한다. 큐비트에 연산을 가하기 위해서는 외부와의 상호작용이 가능해야 하기 때문에 긴 relevant decoherence 시간을 가질 수 있어야 한다.

(4) Universal 양자 게이트를 구성할 수 있어야 한다. 현대 컴퓨터에서의 NAND, NOR 게이트처럼 다른 모든 게이트들을 구현할 수 있는 universal 게이트 set이 필요하다.

(5) 원하는 특정 큐비트에 대한 측정이 가능해야 한다.

위와 같은 조건을 만족시킬 수 있는 양자컴퓨터를 구현하기 위한 다양한 방식이 시도되고 있다. 최초의 양자 컴퓨터라고 주장하는 캐나다 D-WAVE 사의 경우 초전도 회로를 사용하고 있으며 이온 트랩, 양자점, NMR, Cavity QED 방식 등이 존재한다.

현재로써는 양자 컴퓨터가 현대 컴퓨터를 대체 할 수 있는 것은 아니지만 암호 분야에서는 killer application이라 할 수 있는 쇼어 소인수 분해 알고리즘이 존재한다. 1994년에 피터 쇼어가 양자 역학적 성질을 이용하면 소인수 분해를 다항 시간 복잡도로 풀 수 있음을 증명[8]하였다. 따라서 현대 컴퓨터로는 파괴하기 어려운 RSA 공개키 기반의 암호 시스템을 양자 컴퓨터로는 파훼할 수 있음이 증명되었고 양자 컴퓨터의 역할이 주목 받게 되었다. 이러한 알고리즘들이 개발될수록 양자 컴퓨터의 필요성이 대두될 것이다.

나. 양자 오류 정정 부호

1995년 Peter shor가 양자 오류 정정 부호를 구성하는 것이 가능하다는 사실[9]을 발표함으로써 각종 양자 정보 처리 기술이 주목 받게 되었다. 디지털 시스템과 다르게 양자 정보는 복사가 불가능[10]하기 때문에 기존의 오류 정정 부호처럼 간단하게 비트의 정보를 비트로 확장할 수 없다. 따라서 초반에는 기존의 오류 정정 부호를 양자 오류 정정 부호에 변환, 적용하려는 연구가 주를 이루었고, 이후에는 양자 고유의 성질을 이요한 양자 오류 정정 부호들이 연구 되었다.

양자 오류 정정 부호는 양자 정보에 발생하는 Pauli 오류를 정정할 수 있는 기술이다. 단일 큐비트에 대한 Pauli 연산자는 다음과 같다.

$$I = \begin{bmatrix}1 & 0\\ 0 & 1\end{bmatrix}, \quad X = \begin{bmatrix}0 & 1\\ 1 & 0\end{bmatrix}$$
$$Y = \begin{bmatrix}0 & -i\\ i & 0\end{bmatrix}, \quad Z = \begin{bmatrix}1 & 0\\ 0 & -1\end{bmatrix} \tag{6}$$

각각의 Pauli연산자는 서로 anti-commute한 관계로 $\{A,B\} = AB + BA\ (A \neq B)$을 만족한다. 또한 각 연산자는 이진 벡터와 대응이 가능하다.

표 4. Pauli 연산자와 이진 벡터의 대응 관계

$(\mathbb{Z}_2)^2$	Pauli operator
00	I
01	X
11	Y
10	Z

이진 벡터와의 대응 관계를 이용할 경우 Pauli 연산자에서는 곱셈으로 이루어지는 연산을 이진 벡터 상의 modulo 2 연산으로 변환 가능하다.

양자 오류 정정 부호에는 많은 종류의 부호들이 존재하지만 그 중 기본적인 부호라 할 수 있는 안정 부호(Stabilizer code)를 소개한다. 안정 부호는 가장 많이 연구가 되었으며 디지털 시스템에서 쓰이던 선형 오류 정정 부호와 유사한 특징을 가지고 있다.

안정 연산자(stabilizer) 그룹 S는 안정 부호를 구성하는데 가장 중요한 그룹이다. 안정 부호의 코드워드에 대해 안정 연산자는'+1'의 고유값을 갖는다. 따라서 안정 부호의 코드워드는 안정 연산자의 고유 벡터이다.

$$S_i|\psi\rangle = |\psi\rangle \qquad (S_i \in S) \tag{7}$$

안정 연산자 그룹 S은 안정 연산자 생성자(Stabilizer generator)를 통해 표현 가능하다.

$$S = \langle S_1, S_2, \cdots S_m \rangle \tag{8}$$

논리 연산자 $\overline{X}$, $\overline{Z}$는 X, Z Pauli 연산자가 일반적인 큐비트에 작용하는 역할을 코드워드에서 똑같은 작용을 하는 연산자로, 안정 연산자 모두와 commute한 관계를 가진다. 보호하려는 정보가 k큐비트인 경우 $\overline{X}$, $\overline{Z}$는 각각 k개가 존재한다. 논리 $|0\rangle$벡터인 $|\overline{0}\rangle$와 $\overline{X}$를 통해 코드워드들을 생성가능 하기 때문에 k개의 $\overline{X}$을 통해 2^k개의 코드워드를 구성할 수 있다.

안정 부호를 구성하는 단계는 다음과 같다. 양자 상태는 복제가 불가능하기 때문에 k큐비트의 정보를 보호하기 위해서 n큐비트 길이의 부호를 쓸 경우 먼저 n큐비트의 $|0\rangle^{\otimes n}$기저를 준비해야 한다. 이를 안정 연산자를 통해 $|\overline{0}\rangle$로 변환한다.

$$|\overline{0}\rangle = \sum_{S_i \in S} S_i |0\rangle^{\otimes n} \tag{9}$$

안정 연산자를 통해 구성한 $|\overline{0}\rangle$에 $\overline{X}$를 연산해줌으로써 코드워드를 구성할 수 있다.

$$|\overline{c_1 c_2 \cdots c_k}\rangle = \overline{X_1}^{c_1}\overline{X_2}^{c_2}\cdots\overline{X_k}^{c_k}|\overline{0\cdots 0}\rangle \tag{10}$$

큐비트는 이진 정보의 형태이기 때문에 c_i는 $\{0,1\}$중 하나의 값을 가진다. c_i가 1일 경우에는 $|\overline{0}\rangle$에 $\overline{X_i}$가 작용하게 되어 $\overline{0\cdots c_i \cdots 0}\rangle$가 될 수 있다.

예를 들어 5 큐비트 안정 부호[11]의 안정 연산자 생성자는 다음과 같다.

$$XZZXI, IXZZX, XIXZZ, ZXIXZ \tag{11}$$

위의 안정 연산자들을 통해 $|\overline{0}\rangle$을 구성하면 다음과 같다.

$$|\overline{0}\rangle = \sum_{S_i \in S} S_i |0\rangle^{\otimes 5}$$
$$= |00000\rangle + |10010\rangle + |01001\rangle + |10100\rangle + |01010\rangle$$
$$- |11011\rangle - |00110\rangle - |11000\rangle - |11101\rangle - |00011\rangle$$
$$- |11110\rangle - |01111\rangle - |10001\rangle - |01100\rangle - |10111\rangle$$
$$+ |00101\rangle \tag{12}$$

안정 연산자와의 commute 관계를 통해 구한 5 큐비트 안정 부호의 $\overline{X}$는 XXXXX이다. 이를 $|\overline{0}\rangle$에 적용하면 $|\overline{1}\rangle$을 구할 수 있다.

$$|\overline{1}\rangle = \overline{X}|\overline{0}\rangle = XXXXX|\overline{0}\rangle$$
$$= |11111\rangle + |01101\rangle + |10110\rangle + |01011\rangle + |10101\rangle$$
$$- |00100 - |11001\rangle - |00111\rangle - |00010\rangle - |11100\rangle$$
$$- |00001\rangle - |10000\rangle - |01110\rangle - |10011\rangle - |01000\rangle$$
$$+ |11010\rangle \tag{13}$$

이를 통해 5 큐비트를 사용하여 1 큐비트의 정보를 1개의 오류로부터 보호할 수 있는 $[\![5,1,3]\!]$부호를 구성할 수 있다.

다. 양자 난수 발생기

난수는 여러 분야에서 사용되지만 안전한 보안 시스템을 구성하기 위해서 필수적인 요소이다. 예를 들어 암호 키의 생성의 경우 사용된 난수가 얼마나 무작위한지가 안정성을 판단하는데 큰 영향을 미친다. 현재까지는 의사 난수(pseudo-random number)라 하여 프로그램을 통해 만든 난수를 사용하고 있다. 하지만 의사 난수의 경우 난수를 생성하기 위한 초기값을 알게 되면 난수 자체를 계산해낼 수 있다는 문제가 존재하여 완벽한 안전성을 보장하지는 못한다. 이에 반해 양자 역학적 성질을 사용하면 순수 난수(True Random Number)를 만들 수 있어 안정성과 관련된 문제를 해결 할 수 있다. 이러한 장점 때문에 현재 가장 많이 개발 된 양자 시스템인 양자 키 분배 시스템에서 필수적으로 사용된다.

양자 시스템을 통해 난수를 생성하는 방법은 여러 가지 방법이 존재한다. 그 중 가장 간단한 방법은 광자를 50:50 확률로 각각의 출력부에서 검출되는 beam splitter를 통과시키는 것이다. 양쪽 검출기 중 어느 쪽에서 광자가 검출되느냐에 따라 0 또는 1을 결정함으로써 순수 난수를 생성할 수 있다. 이렇게 생성된 순수 난수의 경우 무작위성뿐만 아니라 균등한 분포를 가진다는 장점이 존재한다. 그러나 이 방식은 현재 단일 광자의 생성 및 검출이 매우 어렵고 신뢰도가 떨어지기 때문에 실제 구현 시 효율이 낮다는 단점이 존재한다. 이외에도 반도체의 양자 효과를 이용하거나 원자핵의 방사성 붕괴를 사용한 양자 난수 발생기 등이 존재한다. 현재 군용 통신이나 연구 목적으로 사용되는 양자 난수 생성기는 이미 상용화 되었으며 2014년에 스위스 제네바 대학 연구팀이 스마트폰의 카메라를 통해 양자 난수 발생[12]시킬 수 있는 기술을 발표한 바 있다.

라. 양자 라이더

라이더(LIght Detection And Ranging)란 기본적인 원리는 우리가 잘 알고 있는 레이더(Radio Detction And Ranging)와 동일하지만 레이더에서 사용되는 전자기파 대신 레이저를 사용하는 것을 말한다. 가장 간단한 방식으로는 회전하는 거울에 레이저를 쏘아 물체에 반사된 레이저를 측정하여 물체와의 거리, 형태 등을 측정하는 방법이 있다.

현재 항공기, 위성 등에 설치되어 지형이나 환경 관측을 하는데 주로 사용되고 있으며 최근에는 3D 스캐너 등에서 핵심 기술로 활용되고 있다.

양자 라이더의 경우 레이저 대신 광자를 사용하는 것으로 단일 광자 라이더의 경우 빠르고, 고해상도, 고효율의 단위 측정이 가능하고 최근 3D 스캔에 사용되는 맵핑에 효율적이라는 장점이 존재한다.

Ⅲ. 결 론

본 논문에서는 양자 암호의 기본 원리를 살펴보고 양자 암호의 안전성을 뒷받침 해주는 후처리 알고리즘에 대하여 설명하였다. 또한 양자 통신과 관련된 기술로써 양자 컴퓨터와 양자 오류 정정 부호 그리고 양자 난수 발생기 및 양자 라이더에 대하여 간략하게 살펴보았다.

Acknowledgement

"본 연구는 미래창조과학부 및 정보통신기술진흥센터의 대학 ICT연구센터육성 지원사업의 연구결과로 수행되었음" (IITP-2015-R0992-15-1017)

참 고 문 헌

[1] G. Brassard and L. Salvail, "Secret key reconciliation by public discussion," Lecture Notes in Computer Science, vol. 765, pp. 410 - 423, 1994.

[2] W. T. Buttler, S. K. Lamoreaux, J. R. Torgerson, G. H. Nickel, C. H. Donahue, and C. G. Peterson, "Fast, efficient error reconciliation for quantum cryptography," Physical Review A, vol. 67, no. 5, May 2003.

[3] D. Elkouss, A. Leverrier, R. Alleaume, and J. J. Boutros, "Efficient reconciliation protocol for discrete-variable quantum key distribution," in Information Theory, 2009 IEEE International Symposium, pp. 1879 - 1883. Jul. 2009.

[4] C. H. Bennet, G. Brassard and J. Robert, "Privacy Amplification by Public Discussion" SIAM Journal on Computing Vol. 17 No. 2 Apr. 1988

[5] C. H. Bennet, G. Brassard, C. Crepeau and U. M. Maurer, "Generalized Privacy Amplification" IEEE Transaction on Information Theory Vol. 41 No. 6 Nov. 1995

[6] Richard P. Feynman, "Simulating Physics with Computers" International Journal of Theoretical Physics, VoL 21, Nos. 6/7, 1982

[7] David P. DiVincenzo, "The Physical Implementation of Quantum Computation", arXiv:quant-ph/0002077v3, 13-Apr-2000.

[8] Peter W. Shor, "Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer"arXiv:quant-ph/9508027v2 1994

[9] P. W. Shor, "Scheme for reducing decoherence in quantum computer memory," Phys. Rev. A vol. 52, num. 4, pp. 2493-2496 May. 1995.

[10] Wootters, William; Zurek, Wojciech , " A Single Quantum Cannot be Cloned," Nature vol. 299 pp. 802-803, Oct. 1982.

[11] Daniel Gottesman, "Stabilizer Codes and Quantum Error Correction," arXiv.org, vol. quant-ph. 28-May-1997.

[12] Bruno Sanguinetti, Anthony Martin, Hugo Zbinden, Nicolas Gisin, "Quantum Random Number Generation on a Mobile Phone" Phys. Rev X vol 4, 031056. 2014

약 력

손 일 권

2011년 고려대학교 전자전기전파공학부 학사
2011년~현재 고려대학교 전자전기전파공학부 석박사 통합 과정
관심분야: 통신 시스템, 양자 정보 이론, 양자 오류 정정 부호

이 성 훈

2012년 고려대학교 전자전기전파공학부 학사
2012년~현재 고려대학교 전자전기전파공학부 석박 통합 과정
관심분야: 통신 시스템, 양자 암호

박 주 윤

2011년~현재 고려대학교 전기전자공학부 학사 과정
관심분야: 통신 시스템, 양자 암호

허 준

1989년 서울대학교 공학사
1991년 서울대학교 공학석사
2002년 University of Southern California 공학박사
1991년~1997년 LG전자 책임연구원
2003년~2007년 건국대학교 전자공학과 교수
2007년~현재 고려대학교 전기전자공학부 교수
관심분야: 이동통신 이론, 오류정정부호, 양자암호, 양자오류정정부호